GOLDBERG & GOLDBERG, PLLC
Washington, D.C.
www.goldberglawdc.com

Data Breach 101: The Importance of Involving Counsel Early

DATA BREACH | TECHNOLOGY March 29, 2017

All companies have confidential information they need to protect; for some, that protection is vital to survival. For most, discovery of an intrusion is a crisis. And like many crises, it can be tempting to find the quickest solution: immediately hire investigators and set them loose on the company's computer systems, without considering the collateral effects of acting with abandon.

It is now well known that a recently detected breach is not necessarily (or even likely) a recent breach. Attackers may enter and remain in a network for months or years before detection. And although quick action, upon discovering a breach, is surely necessary, acting too quickly can make matters worse. In particular, directly engaging digital forensics and incident response (commonly known as DFIR) investigators may force the company later to disclose confidential information to law enforcement, government regulators, and private plaintiffs. The problem is that the company may be victimized twice: first by the intrusion, and again by never-ending litigation. The solution is to ensure that DFIR investigators do not work directly for the company, but for company counsel.

The Purpose of Incident Response

Incident response has dual business purposes: (1) to detect, stop, and discover the scope of the intrusion, and (2) to develop evidence to defend the company from subsequent lawsuits. (Although identifying the culprits and assisting law enforcement in their capture are reasonable goals, those goals are not primary business purposes.) This presents a problem: Evidence uncovered by DFIR investigators to stop the intrusion and defend the company may show negligence (or worse), and it may be all discoverable by subpoena in litigation.

Although evidence developed by investigators hired directly by the company may not be protected, evidence uncovered by investigators hired by the company's attorneys may be protected by the attorney-client privilege and the work-product doctrine.

The Attorney-Client Privilege And The Work-Product Doctrine

Communications between an attorney and client are generally protected from disclosure, as are the attorney's mental impressions and other evidence created by the attorney or representatives in anticipation of litigation, by the attorney-client privilege and the work-product doctrine—two related but distinct privileges.

> Only legal counsel can provide the protection of the attorney-client privilege and work-product doctrine—both vital to protecting the company in the immediate wake of the breach and for years after.

The *attorney-client privilege* has been defined to cover any situation in which (1) legal advice of any kind is sought (2) from a professional legal adviser

in his capacity as such, (3) in which the communications relate to that purpose, and (4) were made in confidence (5) by the client or one seeking to become a client. Such discussions (6) are at the client's insistence permanently protected (7) from disclosure by the client or by the legal adviser, (8) except where the protection is waived. 8 J. Wigmore, Evidence § 2292, at 554 (McNaughton rev. ed. 1961); *see, e.g., Fisher v. United States*, 425 U.S. 381, 403 (1976).

A company that anticipates litigation following a breach and acts to defend itself may be able to protect the results of those investigations from disclosure—but only if they are directed by counsel.

The *work-product doctrine* protects documents and other material prepared (1) in anticipation of litigation, (2) by or for a party, or by or for a party's representative. The work-product doctrine protects not only written statements, mental impressions, personal beliefs, and any information assembled by *attorneys* in anticipation of litigation, but also materials prepared at the *direction of an attorney* by paralegals, support staff, consultants, investigators, experts, and the client acting at the attorney's direction. *See, e.g., Hickman v. Taylor*, 328 U.S. 495, 510-11 (1947); Fed. R. Evid. 16(b)(3).

There is also an additional important factor: The attorney-client privilege is incredibly difficult to break; the work-product doctrine may be overcome by showing (i) a substantial need and, (ii) no other access to the information without undue hardship. *Hickman*, 328 U.S. at 509; Fed. R. Evid. 16(b)(3)(A)(ii).

As a result, a company that anticipates litigation following a breach and acts to defend itself, including with DFIR investigations, may be able to protect the results of those investigations from disclosure—but only if they are directed by counsel.

A company may still use internal resources to respond to a breach. But when deciding how to handle the intrusion, the company must take more than cost into account: In addition to the usual chain-of-custody and efficiency concerns, investigations carried out by IT staff in the usual course of their jobs may not be protected.

There is nothing wrong with putting DFIR investigators on alert immediately upon discovery of a breach. And no one wants lawyers to get in the way of technology experts. However, whether internal or external resources are used, the investigation should be undertaken at the high-level direction of counsel.

Disclosure To Government Agencies Or Law Enforcement

Once the investigation is underway, the next step will be to determine whether the company is required to report the breach to a federal or state agency, and whether the company should report it to law enforcement. Federal and state statutes and regulations will govern whether disclosure to one or more agencies is required.

If disclosure is not required by law, whether to make a voluntary disclosure will be a question specific to the business. This is not only a legal question; it is also a public-relations and business question: Law enforcement, once involved, may demand more

"cooperation" than the company may want to provide. And while certain laws (like the CyberSecurity Act of 2015) may provide some protection for cooperation with federal authorities, disclosure of confidential information may waive the attorney-client privilege and may subject the company to other complications, especially when dealing with state authorities. If the company turns over physical items, law enforcement may be in no rush to return them. This may strongly counsel against providing original devices like smart phones or hard drives. Moreover, the progress of the investigation may dictate that any cooperation should be delayed until more information is known.

Contractual Obligations

NExt, non-statutory legal obligations must be considered. Use of cyber-insurance or data-breach insurance may require alerting the company's insurance carrier. Some insurance contracts require immediate carrier notification to trigger coverage or to prevent forfeiture of coverage. At the same time, counsel should review the company's existing list of contractual obligations in the event of a breach: which clients, customers, and business partners must be notified, and exactly how much information must be divulged. If that list has not been prepared in advance, as part of the company's incident-response plan, counsel will be required to take time away from the investigation to review the company's contracts to determine these obligations. At the height of a breach investigation is a difficult time to do pre-breach due diligence.

Moreover, the company must decide whether investigators or attorneys provided by its insurance carrier—sometimes as a condition of coverage for these expenses—will provide the quality or experience the company requires. This is especially problematic when counsel provided by the insurance carrier may be assigned cases in bulk or have little incentive to flag issues that could seriously undermine the company's ongoing business, now and in the future, but that may not be relevant (or could be detrimental) to the insurance company's interest.

At the height of a breach investigation is a difficult time to do pre-breach due diligence.

Disclosure to Collateral Victims

If the intrusion resulted in unintended exposure of the information of customers or clients, the next question is whether or when to disclose the breach to these collateral victims and, by extension, the public. If the company is not otherwise under a legal obligation to disclose, or even if it is, this decision will depend on a combination of contracts, state and federal laws (see above), and the progress of the investigation. Not all mandated disclosures must be immediate. And early disclosure may result in incomplete or inaccurate information, which could cause additional liability, public-relations issues, and poor client relations. Where not legally required, the costs of disclosure may not be covered by insurance; nor may the costs of disclosure obligations that are required only by contract. If the company does disclose the breach, how it is disclosed, and to whom, can greatly affect how clients, business partners, and the public react to the news and view the company's efforts—both to prevent the breach and to stem its damaging after effects.

At Each Stage, Legal Analysis Is Critical

The critical decisions at each stage all have one thing in common—they cannot be made without an incisive view of the company's legal obligations *and* the potentially far-reaching legal implications of the available choices. As with any waterfall of business decisions, the key question will ultimately be what is best for the company. But the company and counsel must be partners in that process—not just to ensure legally mandated steps are taken when required, but also to prevent catastrophic actions or oversights, before they become impossible to reverse. Moreover, this vital fact cannot be ignored: Only legal counsel can provide the protection of the attorney-client privilege and work-product doctrine—both vital to protecting the company in the immediate wake of the breach and for years after.

If you would like to discuss how these issues could affect your business, or if you would like to discuss other contracting issues, contact Richard Goldberg.

Attorney Advertising: This material has been prepared for general informational purposes only and is not intended as legal advice.

GOLDBERG & GOLDBERG, PLLC
1250 Connecticut Avenue NW, Suite 200
Washington, D.C. 20036
(202) 656-5773
www.goldberglawdc.com